Are Conceptualizations of Employee Compliance and Noncompliance in Information Security Research Adequate? Developing Taxonomies of Compliance and Noncompliance

Research-in-Progress

Jeffrey D. Wall
University of North Carolina at Greensboro
jdwall2@uncg.edu

Lakshmi Iyer
University of North Carolina at Greensboro
lsiyer@uncg.edu

A. F. Salam
University of North Carolina at Greensboro
amsalam@uncg.edu

ABSTRACT

This paper offers a grounded theory approach to a review of behavioral information security research. Behavioral information security research is in a nascent state, yet it is growing rapidly due to the importance of information security in organizations. This review examines a particular problem in security research, namely the lack of clear conceptualizations of employee compliance and noncompliance with security policies and norms. This review finds that definitions of compliance and noncompliance are taken-for-granted, which may indicate danger in examining results across studies. Based on existing research of compliance in the information systems field and other fields, this paper identifies four types of compliance and five types of noncompliance along with dimensions of compliance and noncompliance using a grounded theory approach.

Keywords

information security, compliance, noncompliance, taxonomy.

INTRODUCTION

Securing organizational information systems (IS) is an important organizational concern (Richardson, 2009; Richardson, 2011). To protect organizational information from organizational insiders, namely employees, organizations establish security controls (e.g., information security policies, computer monitoring, security training, etc.). Many information security studies examine the behavioral effect security controls have on employees (e.g., Boss, Kirsch, Angermeier, Shingler and Boss, 2009; Bulgurcu, Cavusoglu and Benbasat, 2010; Straub and Nance, 1990). These studies tend to examine compliance and noncompliance with ISPs and behavioral security norms. Based on the review in this paper, we find that many of these studies fail to offer even a simple definition of compliance and noncompliance. By taking the definition of compliance and noncompliance for granted, these studies assume that compliance is a simple concept. However, we know from other fields, such as management and healthcare, that many types of compliance and noncompliance exist (Barofsky, 1978; Dracup and Meleis, 1982; Philippe and Durand, 2011; Smith, Organ and Near, 1983). Unclear conceptualizations of constructs, particularly dependent constructs such as compliance and noncompliance, can limit a field of research (DeLone and McLean, 1992). Therefore, it is essential for IS security studies to clearly identify the type of compliance they examine.

This paper offers a review of conceptualizations of compliance and noncompliance in IS and non-IS literature using a grounded theory approach to provide a taxonomy of compliance and noncompliance that can inform research about information security compliance and noncompliance in organizations. Importantly, security research has begun to develop new conceptualizations of compliance and noncompliance (e.g., Boss et al., 2009; Workman, Bommer and Straub, 2008). However, many information security studies examine broad and ambiguous conceptualizations of compliance, or more commonly, behavioral intentions to comply. This paper attempts to bring these scattered conceptualizations of compliance and noncompliance together into a single taxonomy. Providing a taxonomy of compliance and noncompliance will provide researchers with clear conceptualizations of compliance and noncompliance and will make cross-study examinations more feasible.

To develop the taxonomy, we conducted an electronic search of literature on IS security compliance and noncompliance in the basket-11 journals identified by Clark et al. (2011) (e.g., MISQ, ISR, JMIS, ISJ, EJIS, JAIS, JSIS, JIT, I&M, CAIS, and DSS) using the EBSCO Complete Database. These journals are known for their quality and unique ideas and offer a representative view of the literature. Keywords such as "information security," "compliance," "noncompliance," and "violation" were used in the search. Citations were also examined to find articles in other journals that contribute novel conceptualizations of compliance and noncompliance. Not all articles from the citation lists were included in the review, because the purpose of this paper is to examine differing conceptualizations. To the extent that other articles did not offer new insight beyond what was found in the basket-11 journals, they were excluded from the review. Theoretical sampling of this nature is appropriate for grounded theory studies (Corbin and Strauss, 1990). A total of 27 articles were selected for coding. A grounded theory approach was used to extract important categories and dimensions of compliance and noncompliance from the articles. Axial coding (Corbin et al., 1990) was used to develop the categories of the taxonomies. Importantly, this paper is a research in progress. The taxonomies in this paper are an initial classification based on a primary round of coding. Further coding will be conducted to ensure that the categories and dimensions are adequate and at an appropriate level of abstraction.

This paper directs researchers' attention to the importance of developing sound conceptualizations of a phenomenon before collecting data. This paper also identifies different types of compliance and noncompliance that can be used to ensure that future IS security research is comparable and clearly situated. The remainder of this paper continues as follows. First, the taxonomy of compliance is offered. Second, the taxonomy of noncompliance is offered. Lastly, implications of the taxonomy are discussed and directions for future research are offered.

CONCEPTUALIZATIONS OF COMPLIANCE

Based on initial coding of the literature, two dimensions arose from the literature—goal-orientation and conscious engagement. *Goal-orientation* refers to the extent to which individuals' security behaviors are directed toward accomplishing secure outcomes rather than toward complying with predefined procedures. Thus, goal directed security behaviors are focused on making IS more secure and securing organizational information, whereas procedural behaviors are focused on following policy. Goal directed behaviors, therefore, may go beyond what is required by policy in order to ensure that organizational information is protected. At the core of goal-orientation is motivation. Goal-orientation implies an intrinsic drive to ensure a secure information environment, while procedurally oriented behavior is likely based on extrinsic motivation. *Conscious engagement* refers to the extent to which individuals thoughtfully and diligently engage in secure behaviors. Conscious engagement, however, does not refer to the amount of work an individual must go through in order to complete a security requirement. For example, an individual who habitually completes organizational security requirements may work many hours in performing the security tasks; however, because the behaviors are habitual, by definition they are automatic and require less thoughtful engagement (Verplanken and Orbell, 2003). Although goal-orientation and conscious engagement are related, they are not the same. Goal-orientation captures the motivation to comply, while conscious engagement captures the behavioral enactment of compliance. Although motivation may lead to more conscious engagement, motivation is not actual engagement. Importantly, theoretical dimensions do not need to be orthogonal (Dubin, 1969).

Based on initial coding, we identify four distinct types of compliance—rote, habitually compliance; rote, dutiful compliance; well-intentioned, committed compliance; and proactive, committed compliance. The taxonomy of compliance is presented in Table 1. The sections below describe each type of compliance in greater detail. Because of the confusion that exists in definitions of compliance, we only mention security studies related to each type of compliance if the fit is obvious. Many of the ambiguously defined conceptualizations of compliance are likely to capture elements of several types of compliance.

	Low goal-orientation	High goal-orientation
Low conscious engagement	Rote, habitual compliance	Well-intentioned, committed compliance
High conscious engagement	Rote, dutiful compliance	Proactive, committed compliance

Table 1. Taxonomy of Security Compliance

Rote, Habitual Compliance

Rote, habitual compliance is characterized by low conscious engagement and low goal-orientation. We define rote, habitual compliance as behaviors that align with organizational information security requirements which are nearly routine and automatic to the individual engaging in the behavior. Habitual behaviors are characterized as routine and automatic (Verplanken et al., 2003); therefore, concerted and thoughtful effort may not be required to perform them (Guo, Yuan, Archer and Connelly, 2011). Habitual behaviors may vary by person, as employees' routines may differ. Some behaviors may be so

deeply embedded within the social fabric of an organization they become second nature. This is what Kyngäs et al. (2000) refer to as compliance as ideology.

Few security studies have examined habitual compliance. Vance et al. (2012) is the only study we reviewed that directly measures habitual behavior. They show that habitual behavior is a salient factor in information security policy compliance. Future research might further examine the factors that affect the development of rote, habitual compliance. Managers and researchers may desire to find ways to foster habitual compliance, particularly for security requirements that need frequent, yet thoughtless attention. Such actions might include simple behaviors like logging off of a computer before leaving the computer.

Rote, Dutiful Compliance

Rote dutiful compliance is characterized as being low in goal-orientation, but high in conscious engagement. We define rote, dutiful compliance as deliberate, procedural adherence to organizational information security requirements by an individual who is aware of the security requirements. Though employees who engage in this form of compliance may exert thoughtful effort in fulfilling security requirements, their behavior is likely to be procedural in nature and not directed toward the goal of securing organizational information. Choobineh et al. (2007) suggest that security management in organizations is dominated by a "checklist culture," while it should be dominated by a more proactive and goal directed culture. Procedural rules may lead to procedural behaviors that fail to achieve the initial purpose of the established rule (Choobineh et al., 2007; Lehman and Ramanujam, 2009). Procedural rules emphasize checklist behaviors rather than behaviors that encourage the pursuit of desired outcomes (Lange, 2008; Lehman et al., 2009). Overlap may exist, however, between the outcomes of procedural compliance and goal-directed compliance.

Rote, dutiful compliance may be a remnant of a "checklist culture"; however, this type of compliance may also result from organizational structure and individuals' characteristics and attitudes. For example, extrinsically motivated organizational incentives, such as sanctions and rewards, may lead to positive behavior in the short-term, but may be detrimental to long-term behavior because extrinsic incentives may alter individuals' perceptions of tasks (Bénabou and Tirole, 2003). Thus, sanctions, computer monitoring, and rewards may lead individuals to meet minimum security requirements through rote compliance to security policy while missing the greater goal of the security requirements.

D'Arcy and Herath (2011) note that security deterrence research has mixed results when using compliance, rather than noncompliance, as the dependent variable of the study. They suggest that compliance may not be an appropriate construct for studies employing general deterrence theory. This somewhat limits the examination of different types of security controls (e.g., security training, sanctions, computer monitoring, and moral development) in a single study. We agree that goal-directed compliance may not be useful for deterrence studies; however, we believe that measures of compliance that capture rote, dutiful compliance may provide more consistent findings. Since rote, dutiful compliance is likely to be extrinsically motivated, sanctions may show consistence effects when measured properly. Examining rote, dutiful compliance may open the possibility of reliably studying deterrent and other preventive security controls within a single study.

Well-Intentioned, Committed Compliance

Well-intentioned, committed compliance is characterized by low conscious engagement and high goal-orientation. We define well-intentioned, committed compliance as passive or haphazard engagement in deliberate and thoughtful security behaviors that meet and possibly exceed organizational information security requirements by an individual who is cognizant of and concerned about security outcomes. Well-intentioned, committed compliance may result in compliance with the minimum security requirements of the organization, but may only give rise to occasional proactive security behaviors. The lack of conscious engagement put toward proactive behaviors may result from laziness or limits on time and cognitive attention.

By definition, well-intentioned, committed compliance includes behaviors that at least meet minimum security requirements of the organization. It is likely that well-intentioned, committed compliance exists on a continuum with idle and prioritized negligence, two forms of noncompliance described later. When conscious engagement drops extremely low, employees are likely to become negligent, even in adherence to the minimum security requirements of the organization. Thus, well-intentioned, committed compliance may become negligence. The motivation behind the negligence will determine whether low conscious engagement leads to idle or prioritized negligence.

There are no existing security studies that fit cleanly with this type of compliance though Barofsky (1978) describes compliance of this nature in a healthcare setting, suggesting that patients may desire to be healthy but never put forth the effort to become healthy. Well-intentioned, committed compliance deserves future attention. Most importantly, research

should examine how conscious engagement can be increased and sustained to ensure that well-intentioned behavior becomes proactive, committed compliance.

Proactive, Committed Compliance

Proactive, committed compliance is characterized by high conscious engagement and high goal-orientation. We define proactive, committed compliance as active engagement in deliberate and thoughtful security behaviors that meet and exceed organizational information security requirements by an individual who is cognizant of and concerned about security outcomes. Proactive, committed compliance differs from well-intentioned, committed compliance at the execution stage. At the execution stage, the level of conscious engagement will determine whether behaviors meet minimum security requirements and occasionally exceed them, or consistently exceed them. The goal-directed nature of proactive, committed compliance suggests that employees may seek new and better ways to secure organizational information. Proactive behaviors may include reading security magazines and publications, remaining aware of the latest security software and trends, encouraging management to adopt security software, and other like behaviors.

It is likely that many of the security studies with ambiguous conceptualizations of compliance attempt to capture this type of compliance. Boss et al. (2009) capture proactive, committed security behaviors. They examine precaution taking behavior which they define as "the degree to which individuals perceive they take measures to secure their computers and deal with information security in accordance with prescribed corporate security policies and procedures as well as through individual, proactive actions" (p. 155). Based on the work of Boss et al. (2009), employees may engage in proactive security behaviors. Ng et al. (2009) also examine behaviors that are more proactive in nature. They study protective computer security behavior which they define as "behaviors that will reduce the risk and/or impact of security incidents" (p. 817).

CONCEPTUALIZATIONS OF NONCOMPLIANCE

Based initial coding, we conceptualize noncompliance as consisting of three dimensions—the level of behavioral awareness, the level of maliciousness, and whether the noncompliant actions are intended to benefit oneself or others. *Behavioral awareness* refers to the extent to which individuals are consciously aware of their noncompliant behaviors. *Maliciousness* refers to the extent to which individuals engage in noncompliant behaviors with the intent to cause harm to the organization. And *self-benefitting behavior* refers to noncompliant actions taken with the motive to gratify the individual committing the offense, while *other-benefitting behavior* refers to noncompliant actions taken with the motive to help others (e.g., the organization, clients, or coworkers) or to improve the organizational environment as a whole (e.g., ensuring fair organizational practices). Some overlap exists between these dimensions, as depicted in Table 2. For example, highly malicious behavior is committed with intent to harm. The fact that intention exists in the commission of the behavior, suggests that behavioral awareness must be high. Similarly, behavior that is not malicious and low in behavioral awareness will have no motive attached to the behavior. That is, awareness and intention do not exists in these behaviors; therefore, motives to benefit oneself or others by engaging in the misbehavior are not relevant.

Based on the three dimensions, we identify 5 distinct forms of noncompliance—unintentional misbehavior, idle negligence, prioritized negligence, deviant behavior, and well-intentioned misbehavior. The taxonomy of noncompliance is presented in Table 2. The sections below describe each type of noncompliance in greater detail and provide examples from information security literature.

	Low maliciousness		High maliciousness	
	Self-benefitting	Other-benefitting	Self-benefitting	Other-benefitting
Low behavioral awareness	Unintentional misbehavior			
High behavioral awareness	Idle negligence	Prioritized negligence	Deviant behavior	Well-intentioned misbehavior

Table 2. Taxonomy of Noncompliance

Unintentional Misbehavior

Unintentional misbehavior is characterized by low behavioral awareness and low maliciousness. There is not motive behind the misbehavior; therefore, unintentional misbehavior is neither self- nor other-benefitting. We define unintentional misbehavior as commissive or omissive behavior that is harmful to the security of organizational information unbeknown to the individual engaging in the behavior. Unintentional misbehavior may result from employees who are unaware of security

policies and procedures or from bad habits which employees form. Habitual behavior is automatic and requires less conscious thought (Verplanken et al., 2003); therefore, employees who have bad security habits may not recognize their behavior.

Rote, habitual compliance is likely to be on a continuum with unintentional misbehavior. Unintentional noncompliance may be due to bad security habits. Because habitual behavior is automatic (Verplanken et al., 2003), employees may be unaware or less conscious of their noncompliant actions until after an action is performed. Thus, to the extent that habitual behavior falls within or without the bounds of security requirements, an individual's behavior may be classified as rote, habitual compliance or unintentional misbehavior.

No studies in our review directly examined this form of noncompliance, though it was mentioned by some authors (e.g., Guo et al., 2011). Studies that examine information security policy awareness (e.g., Bulgurcu et al., 2010) are likely to capture some elements of unintentional misbehavior in measures of noncompliance. As research on habit in information security research (e.g., Vance et al., 2012) becomes more prevalent, it may be important to develop measures of noncompliance that clearly capture unintentional misbehavior.

Idle Negligence

Idle negligence is characterized by high behavioral awareness, low maliciousness, and self-benefitting motives. We define idle negligence as the intentional neglect of security behaviors by an individual for reasons that benefit the individual. This type of compliance consists of mostly omissive rather than commissive behavior. Idle negligence is likely the result of laziness, desires to find shortcuts in completing work, desires to enhance personal convenience, or attitudes that security is not important.

Guo et al. (2011) examine nonmalicious security violations, which consist of conscious behavior that is meant to benefit the violator with no direct intent to harm the organization. This places their conceptualization of noncompliance well within idle negligence. Workman et al. (2008) also provide a conceptualization of noncompliance that can be partially categorized as idle negligence. They examine omissive security behavior. However, they do not make a distinction between self-benefitting and other-benefitting motives. Therefore, the omissive behavior in Workman et al. (2008) may also capture elements of prioritized negligence.

Prioritized Negligence

Prioritized negligence is characterized by high behavioral awareness, low maliciousness, and other-benefitting motives. We define prioritized negligence as the intentional neglect of security behaviors by an individual to ensure that time and resources are available for other tasks. This type of compliance also consists of mostly omissive rather than commissive behavior. Prioritized negligence differs from idle negligence in the motive for neglecting a security requirement. Idle negligence results from desires to ease one's own burden, while prioritized negligence results from desires to assist others.

Employees' time is limited and work expectations and work overload are common problems in organizations (Ahuja, Chudoba, Kacmar, McKnight and George, 2007). Employees, therefore, must choose which activities receive their time and attention. Additionally, even if sufficient time existed, humans have limited cognitive capacity (Zhu and Watts, 2010). Individuals' ability to focus attention on multiple items at one time is limited. As such, security activities may suffer from lack of time or attention. Importantly, prioritized negligence does not consist of forgetful behaviors. Forgetful behaviors would fall under unintentional misbehavior. Prioritized negligence occurs when an employee knowingly neglects a security behavior in order to accomplish another task.

As suggested above Workman et al. (2008) provide a conceptualization of noncompliance that partially falls under idle negligence. Similarly, Puhakainen and Siponen (2010) found evidence that work overload hindered compliant behavior, though this was not the focus of their study. Future studies should consider how work requirements in an organization affect employee security behaviors. Future studies that examine this type of noncompliance might explore the position of the employee. It may be that some job positions require greater work and cognitive loads than other positions, increasing the likelihood of prioritized negligence.

Deviant Behavior

Deviant behavior is characterized by high behavioral awareness, high maliciousness, and self-benefitting motives. We define deviant behavior as the intentional commission of insecure information security behaviors by an individual for reasons that benefit the individual. Deviant behaviors include vengeful behaviors, theft, destruction of both physical and informational IS resources, and other intentionally harmful behaviors. Deviant behavior covers behavior committed to harm the organization as a whole or to harm an employee or manager of the organization that has the effect of harming the organization. It is not

concerned, however, with behavior that is harmful to an individual in the organization and not to the organization. Such behavior falls outside the scope of this paper as we are focused on security in organizations and not personal information security.

Many security studies examine this form of compliance. Straub (1990) and Straub and Nance (1990) examine computer abuse, which they define as "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against: hardware (and other physical assets associated with computers, such as theft or damage to terminals, CPU's, disk drives, and printers), programs (such as theft or modification of programs, data (such as embezzlement or modification of data), and computer service (such as unauthorized use of service or purposeful interruption of service)" (Straub, 1990, , p. 257). D'Arcy et al. (2009) and Hovav and D'Arcy (2012) also examine security violations that closely resemble deviant behavior. They examine IS misuse intention, which D'Arcy et al. (2009) define as "an individual's intention to perform a behavior that is defined by the organization as a misuse of IS resources" (p. 81).

Well-intentioned Misbehavior

Well-intentioned misbehavior is characterized by high behavioral awareness, high maliciousness, and other-benefitting motives. We define well-intentioned misbehavior as the intentional commission of insecure behaviors by an individual with the intent of bettering the organization or someone within the organization (e.g., a manager or coworker). Well-intentioned misbehavior differs from deviant behavior based on the motive behind the behavior. Whereas deviant behavior is conducted with the intent to gratify oneself, well-intentioned misbehavior is conducted to help others or improve the organizational environment.

Umphress and Bingham (2011) examine misbehavior in a non-IS setting. They study unethical pro-organizational behaviors. They suggest that employees may knowingly engage in harmful behaviors with the intent of benefiting the organization or a leader of the organization. Ultimately, they suggest that unethical pro-organizational behaviors can lead to serious problems for the organization. This is an interesting direction for future IS research. For example, deviant pro-organizational behaviors may help to explain why doctors are reluctant to follow nationally mandated health privacy standards. It may be that doctors violate these standards with the intent to improve the overall efficiency and quality of health for their patients. Deviant pro-organizational behaviors may also explain security violations related to the Sarbanes-Oxely Act.

Posey et al. (2011) offer an example of this type of noncompliant behavior in IS security literature. They examine justice-related security violations. They introduce justice theory to information security research which suggests that individuals may seek to remedy unfair organizational practices through deviant behavior (Aquino, Tripp and Bies, 2006; Tyler and Blader, 2000). Posey et al. (2011) find that employees may violate security policy as a stand against unfair security practices, such as computer monitoring. Studies that focus on procedural and distributive injustice are likely to fall in this category.

DISCUSSION

This paper has provided a review of security studies to determine what conceptualizations of compliance and noncompliance exist in the literature. Additionally, this paper has extracted important dimensions from these studies and from non-IS literature to form a taxonomy of compliant and noncompliant behaviors. The dimensions described in this paper are mostly derived from previous IS security studies and are only augmented by typologies from other disciplines. The typologies in this paper provide important direction for future research. IS security researchers should carefully select the type of compliance they want to study before collecting data.

Managers should be aware of the type of security compliance they desire to promote in their organizations. The unintentional promotion of one form of compliance could lead to unintended consequences. For example, managers who want committed compliance from employees may find it difficult to attain if managers use extrinsic motivation to entice or coerce compliance. Commitment is more likely to occur when employees are intrinsically motivated (Ryan and Deci, 1985). Extrinsic motivation is more likely to promote rote compliance than true commitment, as commitment requires and inward desire. Additionally, managers should be aware that different forms of noncompliance exist. It is not likely that prioritized negligence should be treated or remedied in the same manner as deviant behavior. Managers' approaches to improving noncompliant behaviors should be tailored toward the particular form of noncompliance an employee engages in. Sanctions and monitoring may be appropriate for deterring employees' harmful intentions, but may do little to promote compliant behaviors when noncompliance is the result of work overload.

Completing the Research

The taxonomy presented above is based on an initial coding of the articles. More rigorous coding practices will be used as the research progresses. Additionally, more non-IS literature will be reviewed and implemented into the development of the taxonomies. The purpose of this paper is to provide a high-level view of types of compliance and noncompliance. As coding continues, we will continue to seek a balance between extremely granular conceptualizations of compliance and noncompliance and broad conceptualizations. Future studies may extend parts of our taxonomy to examine more granular conceptualizations of compliance and noncompliance.

REFERENCES

1. Ahuja, M. K., Chudoba, K. M., Kacmar, C. J., McKnight, D. H., and George, J. F. (2007) IT road warriors: Balancing work-family conflict, job autonomy, and work overload to mitigate turnover intentions, *MIS Quarterly* 31, 1, 1-17.
2. Aquino, K., Tripp, T. M., and Bies, R. J. (2006) Getting even or moving on? Power, procedural justice, and types of offense as predictors of revenge, forgiveness, reconciliation, and avoidance in organizations, *Journal of Applied Psychology* 91, 3, 653-668.
3. Barofsky, I. (1978) Compliance, adherence and the therapeutic alliance: Steps in the development of self-care, *Social Science and Medicine* 12, 5, 369-376.
4. Bénabou, R., and Tirole, J. (2003) Intrinsic and extrinsic motivation, *The Review of Economic Studies* 70, 3, 489-520.
5. Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, W. R. (2009) If someone is watching, I'll do what I'm asked: manditoriness, control, and information security, *European Journal of Information Systems* 18, 151-164.
6. Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly* 34, 3, 523-548.
7. Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. (2007) Management of information security: Challenges and research directions, *Communication of the Association for Information Systems* 20, 1, 958-971.
8. Clark, J. G., Au, Y. A., Walz, D. B., and Warren, J. (2011) Assessing researcher publication productivity in the leading information systems journals: A 2005-2009 update, *Journal of the Association for Information Systems* 29, 459-504.
9. Corbin, J., and Strauss, A. (1990) Grounded theory method: Procedures, canons, and evaluative criteria, *Qualitative Sociology* 13, 3-21.
10. D'Arcy, J., and Herath, T. (2011) A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings, *European Journal of Information Systems* 20, 643-658.
11. D'Arcy, J., Hovav, A., and Galletta, D. (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach, *Information Systems Research* 20, 1, 79-98.
12. DeLone, W. H., and McLean, E. R. (1992) Information systems success: The quest for the dependent variable, *Information Systems Research* 3, 1, 60-95.
13. Dracup, A., and Meleis, A. (1982) Compliance: An interactionist approach, *Nursing Research* 31, 1, 31-36.
14. Dubin, R. (1969) *Theory Building*, (Free Press: New York.
15. Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. (2011) Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, *Journal of Management Information Systems* 28, 2, 203–236.
16. Hovav, A., and D'Arcy, J. (2012) Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea, *Information & Management* 49, 2, 99–110.
17. Kyngäs, H., and Duffy, M. (2000) Conceptual analysis of compliance, *Journal of Clinical Nursing* 9, 1, 5-12.
18. Lange, D. (2008) A multidimensional conceptualization of organizational corruption control, *Academy of Management Review* 33, 3, 710-729.
19. Lehman, D. W., and Ramanujam, R. (2009) Selectivity in Organizational Rule Violations, *Academy of Management Review* 34, 4, 643-657.
20. Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. (2009) Studying users' computer security behavior: A health belief perspective, *Decision Support Systems* 46, 4, 815-825.
21. Philippe, D., and Durand, R. (2011) The impact of norm-conforming behaviors on firm reputation, *Strategic Management Journal* 32, 9, 969-993.
22. Posey, C., Bennett, R. J., Roberts, T. L., and Lowry, P. B. (2011) When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse, *Journal of Information Systems Security* 7, 1, 24-47.
23. Puhakainen, P., and Siponen, M. (2010) Improving employees' compliance through information systems security training: an action research study, *MIS Quarterly* 34, 4, 757-778.
24. Richardson, R. (2009) 14th annual CSI computer crime and security survey, Computer Security Institute, 1-14.
25. Richardson, R. (2011) 15th Annual 2010/2011 Computer Crime and Security Survey, Computer Security Institute, 1-44.

26. Ryan, R. M., and Deci, E. L. (1985) *Intrinsic motivation and self-determination in human behavior*, (Plenum Press: New York, NY.
27. Smith, C. A., Organ, D. W., and Near, J. P. (1983) Organizational citizenship behavior: Its nature and antecedents, *Journal of Applied Psychology* 68, 4, 653-663.
28. Straub, D. W. (1990) Effective IS security: an empirical study, *Information Systems Research* 1, 3, 255-276.
29. Straub, D. W. J., and Nance, W. D. (1990) Discovering and disciplining computer abuse in organizations: A field study, *MIS Quarterly* 14, 1, 45-60.
30. Tyler, T. R., and Blader, S. (2000) *Cooperation in Groups: Procedural Justice, Social Identity, and Behavioral Engagement*, (Psychology Press: Philadelphia, PA.
31. Umphress, E. E., and Bingham, J. B. (2011) When employees do bad things for good reasons: Examining unethical pro-organizational behaviors, *Organization Science* 22, 3, 621-640.
32. Vance, A., Siponen, M., and Pahnila, S. (2012) Motivating IS security compliance: Insights from habit and protection motivation theory, *Information & Management* 49, 190-198.
33. Verplanken, B., and Orbell, S. (2003) Reflections on past behavior: A self-report index of habit strength, *Journal of Applied Social Psychology* 33, 6, 1313–1330.
34. Workman, M., Bommer, W. H., and Straub, D. (2008) Security lapses and the omission of information security measures: A threat control model and empirical test, *Computers in Human Behavior* 24, 2799-2816.
35. Zhu, B., and Watts, S. A. (2010) Visualization of network concepts: The impact of working memory capacity differences, *information Systems Research* 21, 2, 327-344.